TUCA ZBÂRCEA
ASOCIAȚII

15 noiembrie 2019

Știri Legislative

Selecție privind evoluțiile la nivelul UE în domeniul protecției datelor – octombrie 2019

În această ediție:

LEGISLAȚIE

Hotărârea Guvernului nr. 584/2019 pentru modificarea și completarea Hotărârii Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică – CERT-RO

● Monitorul Oficial al României Partea I nr. 673 din 13 august 2019. ● Data intrării în vigoare: 13 august 2019 ● Aplicabilă de la: 27 august 2019

Hotărârea reglementează înființarea CERT RO – în calitate de autoritate competentă la nivel național pentru securitatea rețelei și a sistemelor informatice care asigură servicii esențiale sau servicii digitale în sensul Legii nr. 362/2018.

Regulamentul BNR nr. 2/2019 privind prevenirea și combaterea spălării banilor și finanțării terorismului

● Monitorul Oficial al României Partea I nr. 736 din 9 septembrie 2019. ● Data intrării în vigoare: 9 septembrie 2019 ● Aplicabil de la: 2 octombrie 2019

Regulamentul schimbă regulile privind cunoașterea clientelei. Printre altele, sunt notabile următoarele modificări:

- dispozițiile privind reducerea la minimum a prelucrării datelor – de exemplu, la efectuarea tranzacțiilor ocazionale pot fi prelucrate mai puține date în scopul cunoașterii clientelei; posibilitatea aplicării de măsuri simplificate de cunoaștere a clientelei în situația în care există un risc scăzut de spălare a banilor și finanțare a terorismului;
- instituțiile de credit nu pot iniția, nu pot continua o relație de afaceri sau nu pot efectua o tranzacție ocazională dacă nu pun în aplicare măsuri de cunoaștere a clientelei, inclusiv în cazurile în care nu pot stabili legitimitatea scopului și natura relației de afaceri ori nu pot gestiona adecvat riscul de spălare a banilor și finanțare a terorismului.

SANCȚIUNI PENTRU ÎNCĂLCAREA RGPD

AUTORITATE	AMENDĂ	ÎNCĂLCARE	SECTOR	NR. DE PERSOANE VIZATE	ASPECTE PRINCIPALE	
Autoritatea pentru Protecția Datelor din România (ANSPDCP)	150.000 Euro	Nu au fost implementate măsurile tehnice și organizatorice pentru prevenirea accesului neautorizat și a divulgării datelor cu caracter personal	Servicii financiare	1.177	/	Operatorul trebuie să se asigure că persoanele care acționează sub autoritatea sa prelucrează datele cu caracter personal în limitele atribuțiilor de serviciu ale acestora, și nu în scopuri personale (de exemplu, implementarea de norme interne privind gestionarea datelor, implementarea unor controale adecvate privind conformarea cu regulile interne relevante).
	20.000 Euro	Divulgarea ilegală a datelor cu caracter personal Nu a fost notificată o încălcarea securității datelor cu caracter personal către autoritatea națională de supraveghere	Servicii financiare	1.177	/	Operatorul trebuie să notifice încălcarea securității datelor cu caracter personal autorității de supraveghere fără întârzieri nejustificate (și, dacă este posibil, în termen de cel mult 72 de ore) din momentul în care a luat la cunoștință de aceasta.
	9.000 Euro	Imposibilitatea dovedirii obținerii unui consimțământ explicit Utilizarea unui temei de prelucrare inadecvat	Servicii online	4.357	/ /	Consimțământul trebuie acordat printr-o acțiune neechivocă. Colectarea consimțământului pe baza pasivității persoanei vizate (utilizatori care nu bifează căsuța prin care declară că nu doresc să primească Actualizarea Datelor cu Caracter Personal) nu este adecvată. Operatorii trebuie să se asigure că există un temei juridic adecvat pentru prelucrare – de exemplu transmiterea unei actualizări zilnice cu privire la articolele publicate pe un site de știri nu se poate baza pe necesitatea executării un contract, ci necesită consimțământul persoanelor vizate.
	2.100 Euro	Neluarea în considerare a dezabonării persoanelor vizate (încălcarea prevederilor Legii nr. 506/2004)	Servicii online	1	/	Organizațiile trebuie să implementeze controale adecvate pentru a asigura gestionare retragerii consimțământului (de exemplu, instruirea salariaților în mod adecvat, crearea de fluxuri dedicate retragerii, desemnarea unei persoane care să supravegheze gestionarea cererilor de retragere a consimțământului).
	1.000 Euro	Monitorizarea ilegală prin mijloace de supraveghere video (încălcarea normelor RGPD privind transparența, reducerea la minimum a	Cuptoare industriale și echipamente de încălzire		/	Organizațiile trebuie să poată dovedi că au informat corespunzător persoanele vizate cu privire la monitorizarea prin mijloace de supraveghere video (CCTV).

		prelucrării datelor și legalitatea prelucrării)				
Autoritatea pentru Protecția Datelor din Belgia	10.000 Euro	Nerespectarea principiului reducerii la minimum a prelucrării datelor – solicitarea transmiterii cărții de identitate în format electronic drept condiție obligatorie pentru furnizarea unui serviciu	Comerț online		/	Organizațiile trebuie să ofere opțiuni alternative pentru accesul la un serviciu, în caz contrar consimțământul nu este considerat a fi liber exprimat.
Autoritatea pentru Protecția Datelor din Polonia (UODO)	644.780 Euro	Garanții tehnice și organizatorice necorespunzătoare care au permis accesul neautorizat la baza de date cu clienți a unui magazin online	Comerț online	Aprox. 2,2 mil.	/	Prelucrarea trebuie să aibă loc într-un mod care să asigure securitatea corespunzătoare a datelor cu caracter personal.
	9.380 Euro	Neîncheierea unui contract cu persoana împuternicită conform Art. 28 din RGPD Nerespectarea normelor privind stocarea datelor	Instituții publice		/ /	Dacă prelucrarea se desfășoară în numele unui operator de către o persoană împuternicită de operator, prelucrarea va fi guvernată de un contract sau alt act juridic care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal (în speță, cu societatea care oferea servicii de stocare a datelor și cu societatea care furniza programele software) Operatorul trebuie să efectueze o analiză a riscurilor și să pună în aplicare măsurile de securitate adecvate menționate în art. 32 din RGPD, corespunzătoare riscului de încălcare a drepturilor sau libertăților persoanelor fizice.
Autoritatea pentru Protecția Datelor din Spania (AEPD)	60.000 Euro	Prelucrarea ilegală a datelor ca urmare a neidentificării persoanei vizate	Cosmetice		/	Operatorii trebuie să depună un minimum de diligență în verificarea interlocutorilor pentru a evita deturnarea neautorizată a identității altor persoane.
	36.000 Euro	Prelucrarea ilegală a datelor ca urmare a identificării greșite a persoanei vizate	Servicii de comunicații electronice	1	/	Operatorii trebuie să depună un minimum de diligență în verificarea interlocutorilor pentru a evita prelucrarea neautorizată a identității altor persoane (în speță, consimțământul dat de un membru de familie al persoanei vizate nu a fost considerat valid pentru prelucrarea datelor altor membri ai familiei).
	30.000 Euro	Lipsa unui temei juridic pentru a nu permite	Aviație		/	Societățile trebuie să prevadă un mecanism care să permită utilizatorilor site-ului să-și exprime în mod activ

		utilizatorilor site-ului să refuze modulele cookie				consimțământul pentru diferite categorii de module cookie (acces granular).
	8.000 Euro	Lipsa de cooperare cu autoritatea de supraveghere	Electricitate		/	Nefurnizarea informațiilor solicitate de autoritățile de protecție a datelor poate atrage amenzi.
Autoritatea pentru Protecția Datelor din Suedia	18.630 Euro	Utilizarea ilegală a tehnologiei de recunoaștere facială pentru a monitoriza prezența studenților	Educație		/	În cazul existenței unei relații bazate pe dependență între persoana vizată și operator, trebuie evaluat dacă consimțământul constituie o bază adecvată pentru prelucrare – consimțământul poate fi considerat ca nefiind liber exprimat.
Autoritatea pentru Protecția Datelor din Norvegia	49.100 Euro	Garanții tehnice și organizaționale insuficiente care au permis accesul neautorizat la datele cu caracter personal	Instituție Publică		/	Organizațiile trebuie să permită accesul la datele cu caracter personal doar salariaților cărora le este necesar acest acces pentru îndeplinirea atribuțiilor de serviciu ce le revin.
Autoritatea pentru Protecția Datelor din Bulgaria	2.600.000 Euro	Garanții tehnice și organizatorice insuficiente care au permis diseminarea unei baze de date în mediul online	Agenție Națională de Impozite și Taxe	Aprox. 6 mil	/	În cazul unui atac cibernetic, operatorul trebuie să dovedească că a implementat în prealabil măsuri de securitate organizatorice și tehnice adecvate pentru protejarea datelor cu caracter personal.
	511.000 Euro	Garanții tehnice și organizaționale insuficiente care au permis la diseminarea a 23.000 de istoricuri de creditare	Servicii Financiare	33.000	/	Organizațiile trebuie să pună în aplicare măsuri de securitate organizatorice și tehnice adecvate.
Autoritatea pentru Protecția Datelor din Lituania	7.000 Euro	Nu s-a răspuns la solicitarea persoanei vizate de ștergere a datelor sale cu caracter personal Necooperarea cu Autoritatea de Protecție a Datelor	Comerț online		/ /	Organizațiile trebuie să pună în aplicare o procedură pentru gestionarea cererilor de acces și a altor cereri în materia prelucrării datelor cu caracter personal ale persoanelor vizate Autoritățile pentru protecția datelor iau în considerare cu ocazia stabilirii cuantumului amenzii, inter alia, gradul de cooperare cu autoritatea de supraveghere.
Autoritatea pentru Protecția Datelor din Austria	18.000.000 Euro	Lipsa unui temei legal pentru prelucrarea datelor	Servicii poștale	Aprox. 3 mil.	/	Nu există un temei juridic conform Art. 6 din RGPD pentru crearea de profiluri pentru peste trei milioane de cetățeni austrieci, care să includă informații despre adresele de domiciliu, preferințele personale, obiceiurile și presupusele afinități politice ale acestora și vânzarea profilurilor printre altele, către partide politice și societăți.

	50.000 Euro	Nu a fost desemnat un responsabil cu protecția datelor, deși acest lucru era obligatoriu Prelucrarea s-a bazat în mod eronat pe consimțământ Nu a fost efectuată o evaluare a impactului asupra protecției datelor, deși acest lucru era obligatoriu	Servicii medicale		/	Organizațiile trebuie să verifice dacă prelucrarea necesită desemnarea unui responsabil cu protecția datelor sau o evaluare a impactului asupra protecției datelor.
Autoritatea pentru Protecția Datelor din Germania	14.500.000 Euro	Încălcarea prevederilor RGPD privind reducerea la minim a datelor cu caracter personal prelucrate	Piața Imobiliară		/	Organizațiile trebuie să limiteze datele cu caracter personal prelucrate în ceea privește perioada de stocare și categoriile de date colectate la ceea ce este strict necesar pentru scopurile prelucrării (în speță, informațiile privind salariul, documente de angajare și training, taxe, securitate socială și de sănătate, declarațiile bancare ale chiriașilor nu trebuiau să fie nici colectate inițial și nici stocate pe o perioadă lungă de timp).
	195.407 Euro	Transmiterea de mesaje comerciale deși contul persoanei vizate de pe site-ul operatorului nu mai era activ de mult timp	Servicii de catering	9	/	Organizațiile trebuie să pună în aplicare o Politică de Păstrare a Datelor și să șteargă datele cu caracter personal când perioada de stocare expiră.
Autoritatea pentru Protecția Datelor din Grecia	200.000 Euro	Neluarea în considerare a dezabonării persoanelor vizate de la primirea de mesaje comerciale din partea unor entități terțe	Servicii de comunicații electronice		/	Datele trebuie să fie prelucrate într-un mod care să asigure securitatea corespunzătoare a datelor cu caracter personal și gestionarea adecvată a solicitărilor de dezabonare.
	200.000 Euro	Neconformarea cu dreptul la opoziție și principiul prelucrării cu luarea în considerare a cerințelor privacy by design și by default	Servicii de comunicații electronice	8.000	/	Operatorul trebuie să implementeze măsuri organizaționale și tehnice pentru a permite persoanelor vizate să își exercite dreptul de opoziție la prelucrare și la ștergerea datelor în contextul exercitării dreptului de opoziție.

RECOMANDĂRI

Atunci când „timpul este esențial”: ICO – recomandare privind stabilirea unui termen de răspuns la solicitarea de acces la date formulată de persoanele vizate

Ca urmare a *sentinței CJUE pronunțată în Cauza C-171/03 Maatschap Toeters și M.C. Verberk Productschap Vee en Vleesof*, ICO *și-a actualizat recomandările* privind solicitările persoanelor vizate.

Aspecte principale: Termen de răspuns la o solicitare de acces la date

/ La stabilirea termenului pentru comunicarea unui răspuns la solicitările de acces la date, ziua în care este primită solicitarea de acces la date va fi considerată „Ziua 1”. Astfel, termenul de răspuns la o solicitare de acces la date primită la 29 august se împlinește pe 29 septembrie (și NU pe 30 septembrie).

/ Același sistem trebuie aplicat pentru calculul termenului de răspuns și cu privire la exercitarea celorlalte drepturi de către persoanele vizate, reglementate prin RGPD.

Sunteți pregătiți? Lista de verificare privind implementarea RGPD a Autorității pentru Protecția Datelor din Saxonia Inferioară (**„LfD Niedersachsen”**)

LfD Niedersachsen a publicat o *listă de verificare* privind implementarea RGPD care poate fi utilizată pentru a verifica stadiul conformării cu RGPD.

IAB Tech Lab actualizează specificațiile tehnice pentru Cadrul de transparență și consimțământ al IAB Europe

IAB Europe, principala asociație de la nivel european pentru ecosistemul marketingului digital și al industriei publicitare, în parteneriat cu *IAB Tech Lab*, a anunțat lansarea celei de a doua versiuni a *Transparency and Consent Framework (TCF) (Cadrul de transparență și consimțământ)*.

Manualul responsabilului cu protecția datelor[1]

Manualul este menit să sprijine formarea responsabililor cu protecția datelor **pentru instituțiile publice** în ceea ce privește noile lor atribuții conform RGPD. Deși se adresează instituțiilor publice, aceleași standarde pot fi

[1] Emis de următoarele autorități pentru protecția datelor: Garante per la Protezione dei Dati Personali (Italia), Agencia de Proteccion de Datos (Spania), Agencija za zastitu osobnih podataka (Croația), Comisia pentru Protejarea Datelor cu Caracter Personal (Bulgaria) și Urząd Ochrony Danych Osobowych (Polonia).

luate în considerare și în cazul responsabililor cu protecția datelor din **sectorul privat**. Manualul poate fi accesat *aici*.

Aspecte principale:

/ Cunoștințele de specialitate ale responsabililor cu protecția datelor se referă la:

(a) experiență privind legislația europeană din domeniul confidențialității și al protecției datelor, inclusiv experiență în IT și securitate cibernetică; și

(b) o bună înțelegere a modului în care funcționează instituția [în cadrul căreia este desemnat responsabilul cu protecția datelor] și a activităților sale de prelucrare a datelor cu caracter personal și abilitate de interpretare a normelor relevante privind protecția datelor în acest context.

/ Deținerea de cunoștințe tehnice privind sistemele informatice implică o bună înțelegere a terminologiei din domeniul IT, a practicilor informatice și a formelor diferite de prelucrare a datelor. Spre exemplu, un responsabil cu protecția datelor trebuie să cunoască, spre exemplu: sistemele de administrare și exploatare a datelor, tipul de software utilizat, sistemele de stocare a fișierelor și datelor, precum și cerințele politicilor de confidențialitate și securitate (criptarea datelor, semnături electronice, elemente biometrice etc.)

Recomandările Comisarului landului Schleswig-Holstein responsabil pentru protecția datelor („**ULD**”) pentru prevenirea încălcărilor securității datelor – versiune disponibilă doar în limba germană

ULD a publicat câteva *recomandări* pentru prevenirea încălcărilor securității datelor. Printre altele, acestea se referă la necesitatea utilizării criptării în situația în care site-urile afișează formulare pentru colectarea datelor clienților.

Comisarul pentru informații („**IC**”) al Insulei Man: recomandări privind utilizarea sistemelor de supraveghere video

IC a publicat un set de *recomandări privind utilizarea sistemelor de supraveghere video* de către operatori.

Aspecte principale:

/ Camerele de supraveghere video trebuie să fie amplasate iar capturarea imaginilor să fie limitată, astfel încât să nu acopere zone care nu sunt relevante pentru scopul prelucrării (spre exemplu, proprietăți private ale persoanelor fizice).

/ Specificațiile tehnice ale sistemului trebuie să asigure o calitate adecvată a imaginilor pentru scopul avut în vedere.

/ Semnele/pictogramele legate de camerele video trebuie: (i) să fie vizibile în mod clar și să fie inteligibile; (ii) să menționeze detalii privind organizația care utilizează sistemul, scopul/scopurile utilizării sistemului de supraveghere video și persoana de contact cu privire la acest sistem – în situația în care acestea nu reies din context; și (iii) să fie de dimensiuni adecvate.

/ De asemenea, divulgarea imaginilor din sistemul de supraveghere video trebuie să fie controlată și să respecte scopul pentru care a fost instalat sistemul. Cu toate acestea, persoanele fizice au dreptul de a solicita copii ale imaginilor cu propria persoană.

Autoritatea pentru Jocuri de Noroc din Malta: Recomandări privind comunicările comerciale

Aceste recomandări constituie un ghid practic pentru persoanele care comercializează jocuri de noroc licențiabile și persoanelor care colaborează în orice fel sau care prestează orice serviciu, inclusiv servicii de marketing sau de promovare pentru sau pe seama acestor persoane.

Declarația CNIL (Autoritatea pentru Protecția Datelor din Franța): Înregistrarea convorbirilor telefonice și a utilizării calculatorului de către angajați

CNIL a publicat o *declarație* privind înregistrarea convorbirilor telefonice și a utilizării calculatorului de către angajați (disponibil numai în limba franceză).

Aspecte principale:

/ De regulă, prelucrarea informațiilor de pe capturile de ecran alături de înregistrarea convorbirilor telefonice este considerată disproporționată atunci când această prelucrare este folosită în alte scopuri decât formarea profesională a angajaților (de exemplu, evaluarea personalului, combaterea fraudei interne, etc.)

Nota tehnică a AEPD (Autoritatea pentru Protecția Datelor din Spania): Responsabilitatea proactivă în aplicațiile mobile

AEPD a publicat o *notă tehnică* pentru prezentarea pe scurt a practicilor RGPD pentru organizațiile responsabile cu prelucrarea în aplicația mobilă și dezvoltatorii acestor aplicații.

Aspecte principale:

/ Informațiile RGPD trebuie să fie disponibile atât în magazinul virtual de aplicații (app store) cât și în aplicație, într-o limbă corespunzătoare pentru utilizatorul vizat;

/ Organizațiile care acționează în calitate de operatori pentru datele din aplicații trebuie să precizeze în contractele privind prelucrarea datelor, obligația persoanelor împuternicite de a asigura bunele practici și de a lua în calcul regulile Privacy by design and by default chiar de la momentul dezvoltării aplicațiilor;

/ Trebuie avute în vedere, în special, următoarele practici: gradul de detalii pentru gestionarea accesului acordat la resursele de sistem protejate; respectarea preferințelor de confidențialitate ale utilizatorului; evitarea transferului de date către prestatori de servicii de analiză a pieței (analytics) și publicitate în momentul în care utilizatorul accesează aplicația fără oferi utilizatorilor posibilitatea de a accesa acele date ori de a își modifica opțiunile; utilizarea unor metode avansate pentru criptarea comunicațiilor.

Garante (Autoritatea pentru Protecția Datelor din Italia): Codul de conduită pentru analiza riscului de credit pentru sistemele de informații private

---

Aspecte principale:

/ Prelucrarea datelor cu caracter personal cuprinse într-un SIC poate fi realizată exclusiv în scopul evaluării, recrutării sau gestionării unui risc de credit, al evaluării gradului de seriozitate și punctualitate în efectuarea plăților părții interesate – în vederea împiedicării riscului de fraudare și furt de identitate;

/ Prelucrarea datelor cu caracter personal este necesară pentru îndeplinirea intereselor legitime ale participanților la utilizarea SIC în scopurile menționate în CoC;

/ Informațiile negative despre credite în legătură cu întârzierile la plată, regularizate ulterior, pot fi păstrate într-un SIC cel mult: a) douăsprezece luni de la data înregistrării datelor în legătură cu regularizarea întârzierilor care nu depășesc două rate sau luni; b) douăzeci și patru de luni de la data înregistrării datelor în legătură cu regularizarea întârzierilor care depășesc două rate sau luni.

JURISPRUDENȚA UE

Decizia CJUE în Cauza Google vs. CNIL

La data de 24 septembrie 2019 CJUE a decis că, în momentul în care primește o cerere de a ascunde paginile de internet care conțin informații despre o persoana vizată, din partea acelei persoane vizate conform RGPD, operatorul motorului de căutare nu are obligația de a ascunde paginile de internet în toate versiunile motorului, ci numai în versiunea corespunzătoare pentru toate Statele Membre UE.

Decizia preliminară a CJUE privind Articolul 15 alineatul (1) din Directiva 2000/31/CE

Pe 3 octombrie 2019, CJUE a emis o *decizie preliminară* privind interpretarea Articolului 15 alineatul (1) din Directiva 2000/31/CE a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societăților informaționale, în special privind comerțul electronic pe piața internă („Directiva privind comerțul electronic")

Aspecte principale:

/ A decis că Directiva privind comerțul electronic, în special Articolul 15 alineatul (1), trebuie interpretat în sensul că nu se opune posibilității ca o instanță dintr-un stat membru:

/ să oblige un furnizor de servicii de stocare-hosting să elimine informațiile pe care le stochează și al căror conținut este identic cu cel al unei informații declarate anterior ilicite sau să blocheze accesul la acestea, oricare ar fi autorul cererii de stocare a acestor informații;

/ să oblige un furnizor de servicii de stocare-hosting să elimine informațiile pe care le stochează și al căror conținut este echivalent cu cel al unei informații declarate anterior ilicite sau să blocheze accesul la acestea, în măsura în care supravegherea și căutarea informațiilor vizate de o astfel de somație sunt limitate la informații care transmit un mesaj al cărui conținut rămâne în esență neschimbat în raport cu cel care a condus la constatarea caracterului ilicit și care cuprind elementele specificate în somație, iar diferențele din formularea acestui conținut echivalent în raport cu cea care caracterizează informația declarată anterior ilicită nu sunt de natură să îl constrângă pe furnizorul serviciilor de stocare-hosting să efectueze o apreciere autonomă a acestui conținut și

/ să oblige un furnizor de servicii de stocare-hosting să elimine informațiile la care se referă somația sau să blocheze accesul la acestea la nivel mondial în cadrul dreptului internațional relevant.

SFATUL NOSTRU

Oportunități profesionale pentru candidați

În cazul în care candidatul nu este selectat pentru etapa următoare a procesului de recrutare, puteți lua în considerare următoarele:

/ Informați candidații într-un mod clar și complet înainte ca aceștia să-și depună candidatura cu privire la modul în care vor fi utilizate datele lor în cadrul recrutării.

/ În special:

(a) Comunicați candidaților dacă intenționați să utilizați CV-ul lor și pentru alte posturi decât cele indicate în anunțul de recrutare.

(b) Informați candidații că au dreptul de a se opune, fără a prezenta vreo justificare, utilizării pe viitor a CV-ului lor pentru alte posturi disponibile. Menționăm că opoziția candidaților poate fi exprimată și indirect, de exemplu prin precizarea în mod clar a faptului că sunt interesați exclusiv de postul pentru care a fost publicat anunțul sau prin indicarea postului vizat.

/ Dacă intenționați să utilizați CV-ul și pentru ocuparea altor posturi:

(a) Informați candidații cu privire la această intenție; în special, indicați perioada aplicabilă pentru această utilizare viitoare și măsurile de siguranță implementate în acest context (de ex., stocarea inactivă – precum arhivarea, folosirea unui pseudonim/criptarea, accesul limitat etc.); și

(b) Obțineți acordul candidaților pentru această utilizare.

Editori

Avocații Țuca Zbârcea & Asociații dețin o experiență notabilă în domeniul **Protecției Datelor cu Caracter Personal**, personal/ RGPD, atât la nivel intern, cât și în alte țări, activând în mai multe sectoare comerciale, precum: telecomunicații, servicii financiare (bancare, de asigurări, pensii, etc.), sistemul de sănătate, farmacie, e-comerț, IT, energie, sectorul alimentar, etc. Serviciile noastre acoperă toate aspectele legate de protecția datelor cu caracter personal, de la notificarea autorității locale de reglementare (Autoritatea Națională pentru Supravegherea Datelor cu Caracter Personal – **„ANSPDCP”**) cu privire la diverse aspecte (precum notificarea încălcărilor obligațiilor de protecție a datelor cu caracter personal, consultanță în vederea evaluării impactului în ceea ce privește protecția datelor în cazurile cu risc ridicat, consultanță în ceea ce privește evaluările interesului legitim în situații sensibile, etc.), până la realizarea unor analize complexe pe probleme sensibile din domeniul protecției datelor cu caracter personal / RGPD, cum ar fi: implementarea completă a RGPD; realizarea unor evaluări ale impactului asupra protecției datelor (DPIA) și evaluări ale intereselor legitime (LIA); monitorizarea salariaților; geolocație; istoricul apelurilor; fișiere de tip *cookie*; prelucrarea datelor de trafic; implementarea soluțiilor de *cloud computing;* auditarea persoanelor împuternicite să prelucreze datele cu caracter personal; partajarea datelor cu caracter personal; negocierea termenilor relevanți ai contractelor de prelucrare a datelor (CPD); codurile de conduită din industrie; traininguri RGPD/ protecția datelor; soluționarea plângerilor depuse de persoanele vizate, etc. Cei interesați de noutățile din acest domeniu pot accesa blogul Țuca Zbârcea & Asociații – *dataprivacyblog.tuca.ro*

Horia Ispas
Partner
+40 37 413 63 16
horia.ispas@tuca.ro

Ciprian Timofte
Managing Associate
+4 021 204 88 90
ciprian.timofte@tuca.ro

TUCA ZBARCEA ASOCIATII
Șos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro